Title	**Demonstrate knowledge of electronic security system design**		
Level	**4**	**Credits**	**10**

Purpose	This unit standard is intended for the training and assessment of people working in or intending to work in the electronic security industry and covers the knowledge and application of electronic security systems. People credited with this unit standard are able to demonstrate knowledge of: – evaluation requirements to mitigate risks in a given scenario; – electronic security intruder alarm system design; – electronic security access control system design; – electronic security surveillance system design; – integrated electronic security power supply system design; and – wireless technology as used in a security system design.

Classification	Electronic Engineering > Electronic Security

Available grade	Achieved

Guidance Information

1 This unit standard has been developed for learning and assessment off-job.

2 Persons working or intending to work as a security officer or in related security employment may require a Security Guards Licence or, if an employee of a Security Guard Licence holder, a Certificate of Approval to be the Responsible Employee of a Security Guard. These licences are issued by the Private Security Personnel Licensing Authority available through: www.justice.govt.nz/tribunals/licences-certificates/pspla/.

3 Definitions
AV – audio visual.
CIF – common interchange format.
Component – any device, module, part, or sub-system of any security system.
DVR – digital video recorder.
EDR – emergency door release.
Environmental – may include sunlight, heat sources, halogen lights, pets, drafts, insects, rodents, weather, electrical interference, lightning, radio interference.
Industry practice – practice used and recommended by organisations involved in the electrotechnology industry.
Multi-door installation – multiple doors controlled by a single access control system.

NVR – network video recorder.
PIR – passive infra-red.
POE – power over ethernet.
PTZ – pan tilt zoom.
Resolution – covers range from CIF to megapixel.
REX – request to exit.
Risk – the chance of something happening that will have an impact upon objectives, measured in terms of consequences and likelihood.
Safe working practices – work practices designed to prevent personal injuries and damage to equipment and plant. This includes practices relating to personal attire and use of safety clothing and equipment, use of machinery and tools, and handling of materials and waste.
Threats – things or actions that present risks to people, assets, or events, and which, if untreated, may result in harm, fear, disruption, loss, damage, compromise or destruction.
Wi-Fi – Wireless Internet - a trademark of the Wi-Fi Alliance.

4 References
Building Act 2004;
Electricity Act 1992;
Health and Safety at Work Act 2015;
Privacy Act 1993;
Private Security Personnel and Private Investigators Act 2010;
Telecommunications Act 2001;
AS 2201.2-2004, *Intruder alarm systems – Monitoring centres;*
AS 2201.3:1991, *Intruder alarm systems, detection devices for internal use*;
AS 2201.4:1990, *Intruder alarm systems – Wire-free systems installed in client's premises*;
AS/NZS 2201.1:2007, *Intruder alarm systems – Client's premises—Design, installation, commissioning and maintenance*;
AS/NZS 2201.5:2008, *Intruder alarm systems – Alarm transmission systems*;
AS/NZS 3000:2007, *Electrical installations (known as the Australian/New Zealand Wiring Rules)*;
IEC 60839-11-1, *Electronic access control systems - System and components requirements*;
IEC 60839-11-2, *Electronic access control systems - Application guidelines*;
NZS 4512:2010, *Fire detection and alarm systems in buildings*;
New Zealand Security Association (Inc), Codes of Practice available at https://security.org.nz/;
New Zealand Telecommunications Forum Incorporated cabling requirements;
Local territorial authority requirements;
and all subsequent amendments and replacements.

5 Guidelines for connection of intruder alarm systems to telephone lines are contained in *Access Standards Newsletters* issued periodically by Spark NZ Ltd, available from www.telepermit.co.nz.

6 Range
a Candidates may refer to current legislation and Standards during assessment.
b Demonstration of safe working practices in accordance with *safe and sound practice* are essential components of assessment of this unit standard.
c All activities and evidence presented for all outcomes and performance criteria in

this unit standard must be in accordance with:
i legislation;
ii policies and procedures;
iii ethical codes;
iv Standards;
v applicable site, enterprise, and industry practice; and,
vi where appropriate, manufacturer instructions, specifications, and data sheets.

Outcomes and performance criteria

Outcome 1

Demonstrate knowledge of evaluation requirements to mitigate risks in a given scenario.

Range evidence of three different scenarios is required.

Performance criteria

1.1 Explain the relationships between risks, threats, and vulnerabilities in terms of people, property and information.

1.2 Describe options to manage the identified risks.

1.3 Explain the need and techniques used for encryption and authentication in a security system.

1.4 Identify requirements under the Privacy Act for data storage, surveillance, and signage as pertaining to electronic security systems.

Outcome 2

Demonstrate knowledge of electronic security intruder alarm system design.

Performance criteria

2.1 Explain programmable functions in terms of intruder alarm systems, with reference to their suitability for given situations.

Range functions may include but are not limited to – points and/or zones, areas, partitioning, common areas, zone doubling, duress, user authorisation, late working, auto arming, stay mode, bypass, isolate, walk test, time zone, entry delay, exit delay, siren time; evidence of five functions is required.

2.2 Explain the main management functions of an intruder alarm system.

Range functions may include but are not limited to – user programming, alarm activity reporting, user activity reporting, system time programming, system status, system test, off-site monitoring; evidence of three functions is required.

2.3 Explain safety and local body regulations in relation to noise level of internal and external audible devices.

2.4 Explain influences that may impact on component performance.

Range may include but is not limited to – radio transmissions, building fit-out, electromagnetic interference, humidity, moisture, insects, vermin, birds, temperature, wind, rain, lightning, power supply; evidence of five is required.

2.5 Identify and describe the suitability of components for given scenarios.

Range components may include but are not limited to – audible devices, communication devices, PIR detector, microwave detector, point-to-point beam, dual and quad technology detector, reed switches, seismic sensors, glass break detectors, perimeter detectors, personal alarms;
evidence of three scenarios is required.

2.6 Design electronic intruder alarm systems to meet given scenarios.

Range includes but is not limited to – design specification, site plan, equipment and cable schedules, system programming requirements, supporting documentation;
evidence is required for one domestic site and one light commercial site.

Outcome 3

Demonstrate knowledge of electronic security access control system design.

Performance criteria

3.1 Identify and describe the suitability of components for given scenarios.

Range components may include but not limited to – electric strikes, electric mortise locks, electromagnetic locks, v-lock, turnstiles, vehicle barrier arm; cable transfer hinges, egress switches, point-to-point beam, vehicle detection loop, credential reader (key, card, tag, biometric, mobile phone, wireless device), radio and infra-red transmitters, mechanical door closer, automatic door closer, auto door, vehicle arresting devices, REX, EDR, fire release;
evidence of three scenarios is required.

3.2 Describe access control system management functions.

Range functions may include but are not limited to – card programming, alarm activity reporting, card user activity reports, temporary card issue, holiday time scheduling, lost card control, fire evacuation reporting, user grouping, authorisation levels, lift floor levels, global access, restricted access, anti-passback, two person rule, blocked card, expiry dates, time schedules, area lockdown; evidence of five is required.

3.3 Describe safety issues relating to emergency egress.

Range includes but is not limited to – fire alarm override, building code compliance, emergency evacuation, lift access control, EDR, emergency break glass, lock type selection, emergency key override.

3.4 Explain influences that may impact on component performance.

Range may include but is not limited to – radio transmissions, building fit-out, electromagnetic interference, humidity, moisture, insects, vermin, temperature, rain, wind, air pressure loading, building movement, door specification, power supply;
evidence of five is required.

3.5 Design access control systems to meet given scenarios.

Range includes but is not limited to – design specification, site plan, equipment and cable schedules, system programming requirements, supporting documentation;
evidence is required for one single-door installation and one multi-door installation.

Outcome 4

Demonstrate knowledge of electronic security surveillance system design.

Performance criteria

4.1 Explain surveillance system functions and describe their suitability for given scenarios.

Range may include but is not limited to – frames per second, images per second, motion detection, privacy zone, CIF, pixel, resolution, image compression method, text insertion, archive, lenses, alarm triggers, event programming, image sensor, analytics, audio, intercom systems;
evidence of three scenarios is required.

4.2 Describe component performance, interference, and lighting scenarios.

Range may include but is not limited to – illumination levels, shadows, direct sunlight, glare, rapid light fluctuation, scene contrast, colour rendering, lamp types, dimming, bandwidth requirement, obstructions, audio quality and sensitivity;
evidence of three scenarios is required.

4.3 Identify and describe the suitability of different surveillance system technologies for given scenarios.

Range may include but is not limited to – cameras, fixed and auto iris lenses, DVR, NVR, matrix switch, virtual matrix, PTZ, megapixel, server and POE switches, AV recording;
cameras may include but are not limited to – dome, full body, infrared detection;
evidence of three scenarios is required.

4.4 Design surveillance systems to meet given scenarios.

Range includes but is not limited to – design specification, site plan, equipment and cable schedules, system programming requirements, supporting documentation;
evidence is required for one domestic installation and one light commercial installation.

Outcome 5

Demonstrate knowledge of integrated electronic security power supply system design.

Performance criteria

5.1 Describe advantages and disadvantages of power supply types.

Range power supply types may include but are not limited to – linear, switchmode, POE;
evidence of two advantages and two disadvantages for each is required.

5.2 Describe power supply management functions.

Range mains fail, low battery, battery charging.

5.3 Explain advantages and disadvantages of centralised and distributed power supply systems.

Range includes but is not limited to – fire alarm override, monitoring functions, mains reticulation, voltage drop.

5.4 Describe characteristics of three different backup battery technologies.

5.5 Explain environmental considerations that may affect component performance.

Range includes but is not limited to – heat, corrosion, humidity, airflow.

5.6 Design power supply system to meet given outcomes for an electronic security system for given load requirements.

Range power supply size, battery capacity, monitoring, battery recharge times;
evidence of two scenarios is required.

Outcome 6

Demonstrate knowledge of wireless technology as used in a security system design.

Performance criteria

6.1 Explain wireless system design as applied to an electronic security system.

Range may include but is not limited to – line of sight, transmitter range, interference, spectrum analysis, bit error rate, radio spectrum, environmental considerations, mounting considerations, building structures, Bluetooth, Wi-Fi.

6.2 Describe safety issues relating to wireless systems.

Range electromagnetic radiation, safe working practises, exposure limits.

6.3 Design wireless systems for a given scenario.

Range may include but is not limited to – design specification, site plan, equipment and cable schedules, programming requirements, manufacturer documentation, power requirement.

Replacement information	This unit standard replaced unit standard 27178.

Planned review date	31 December 2023

Status information and last date for assessment for superseded versions

Process	Version	Date	Last Date for Assessment
Registration	1	24 January 2019	N/A

Consent and Moderation Requirements (CMR) reference	0003

This CMR can be accessed at http://www.nzqa.govt.nz/framework/search/index.do.

Comments on this unit standard

Please contact The Skills Organisation reviewcomments@skills.org.nz if you wish to suggest changes to the content of this unit standard.